UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,826	03/26/2004	Blayn W. Beenau	60655.8700	2825

20322 7590 11/29/2005

SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 850040001

EXAMINER	
NGUYEN, NAM V	

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/708,826	BEENAU ET AL.	
	Examiner	Art Unit	
	Nam V. Nguyen	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/20;4/9;3/26/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The application of Beenau et al. for a "method and system for facial recognition biometrics on a fob" filed March 26, 2004 has been examined.

This application is a CIP of 10/340,352 filed January 10, 2003, which is a CIP of 10/192,488 filed July 9, 2002, which claims the benefit of 60/304,216 filed July 10, 2001 and said 10/340,352 filed January 10, 2003, which is a CIP of 10/318,432 filed December 13, 2002 and is a CIP of 10/318,480 filed December 13, 2002, and claims benefit of 60/396,577 filed July 16, 2002.

Claims 1-47 are pending.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The current abstract using phrase "the present invention" and "the invention" is implied and should be avoided. See MPEP 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-47 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 1, the phrase "said system comprising:" is confusing and unclear. It is not understood what is meant by such a limitation. Is the system a transponder-reader transaction system or a biometric security system? What are the different between a system, a transponder-reader transaction system and a biometric security system? Claims 2-9 are rejected for their dependence on Claim 1 and include the same limitations of Claim 1 without correcting the ambiguity.

In claim 1, the phrase "a device configured to verify said proffered facial scan sample to facilitate a transaction" is confusing and unclear. It is not understood what is meant by such a limitation. What is a device? Is a device in a reader or in a transponder or in a facial scan sensor? Where is this limitation supported by specification?

In claim 3, the phrase "wherein said facial scan sensor is configured to facilitate a finite number of scans" is confusing and unclear. It is not understood what is meant by such a

limitation. What facilitate a finite number of scan mean? What is a finite number? Where is this limitation supported by specification?

Claim 7 recites the limitation "remote database" in line 2. There is insufficient antecedent basis for this limitation in the claim. Also the phrase "wherein said remote database is configured to be operated by an authorized sample receiver" is confusing and unclear. It is not understood what is meant by such a limitation. What exactly is an authorized sample receiver? Is an authorized sample receiver of a reader or an authorized user? Where is this limitation supported by specification?

In claim 16, the phrase "wherein a facial scan sample is primarily associated with at least one of first user information,…, and wherein a facial scan sample is secondarily associated with at least one of second user information" is confusing and unclear. It is not understood what is meant by such a limitation. What is the different between primarily and secondarily? What is a user information? What is a first and second information? Is primarily and secondarily includes the same or identical personal information? Where is this limitation supported by specification?

In claim 17, the phrase "configured to begin mutual authentication upon verification of said proffered facial scan sample" is confusing and unclear. It is not understood what is meant by such a limitation. What is configuring to begin mutual authentication? Is the reader authenticated the transponder, vice versa or both? Where is this limitation supported by specification?

In claims 20-21, the phrase "wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure" is confusing and unclear. It is not understood what is meant by such a limitation. What is the device do? Is the device verify or configure? Where is this limitation supported by specification?

In claim 22 and 35, the phrase "detecting a proffered biometric at a sensor communicating with said system to obtain a proffered biometric sample" is confusing and unclear. It is not understood what is meant by such a limitation. Is a sensor detecting a proffered biometric sample? Is the sensor locate in the transponder, in a reader or in a system? What is the different between a proffered biometric and a proffered biometric sample? Where is this limitation supported by specification? Claims 22-34 and 36-47 are rejected for their dependence on Claims 22 and 35 and include the same limitations of Claims 22 and 35 without correcting the ambiguity.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 10-29, 32-43, and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kita (US# 6,703,918) in view of Black (US# 6,307,956).

Referring to claims 1, 22 and 35, Kita discloses a method and a transponder-reader transaction system (i.e. an authentication system) (see Figures 3, 10-11, 14-15, 20 and 24-25) configured with a biometric security system (1) (i.e. a portable information equipment), said system comprising:

a transponder (171) (i.e. a portable information equipment) configured to communicate with a reader (191) (i.e. authentication device) (column 10 line 63 to column 12 line 67; see Figure 10-11); a reader (191) (i.e. authentication device) configured to communicate with said system (197) (i.e. system or server) (column 12 line 6 to 67; see Figure 11); a biometric sensor (8 or 10) configured to detect a proffered biometric scan sample (i.e. authentication data), said biometric scan sensor (8 or 10) configured to communicate with said system (197) (i.e. system or server); and a device (152) (i.e. a control circuit) configured to verify said proffered biometric scan sample (i.e. authentication data) to facilitate a transaction (column 19 line 48 o 67; see Figures 24-25).

However, Kita did not explicitly disclose a facial scan sensor configure to detect a proffered facial scan sample.

In the same field of endeavor of biometric identity verification system, Black teaches that a facial scan sensor (2) (i.e. a facial imaging) configure to detect a proffered facial scan sample (i.e. biometric properties) (column 4 lines 31 to 43; see Figures 1-6) in order to identify the identity of a person using the biometric means for use at point of sale.

One of ordinary skilled in the art recognizes using a facial imaging in a mobile computing device of Black in a portable information equipment of Kita because Kita suggests it is desired to provide that the portable information equipment includes plurality of biometric sensors to authenticate the user (column 10 line 62 to column 12 line 40; column 14 lines 42 to 61; see Figures 10-15) and Black teaches that the mobile computing device includes a plurality of biometric sensors including a facial imaging (i.e. a camera) to identify the user in the identity verification system in order to increase security for e-commerce. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to using a facial imaging in a mobile computing device of Black in a portable information equipment of Kita with the motivation for doing so would have been to secure the verification of the user in the identity verification system for e-commerce.

Referring to Claims 2 and 36, Kita in view of Black disclose the method and the transponder-reader transaction system of claims 1and 35, Kita discloses wherein said sensor (155) (i.e. organic measurement sensor) is configured to communicate with said system (197) via at least one of a transponder (171) (column 12 line 6 to 40; see Figures 10-15)

Referring to Claims 3 and 39, Kita in view of Black disclose the method and the transponder-reader transaction system of claims 1and 35, Kita discloses wherein said facial scan sensor (176) is configured to facilitate a finite number of scans (column 4 line 20 to column 5 line 9; column 10 line 62 to column 11 line 61; see Figures 1-3 and 10-15).

Referring to Claims 4 and 40, Kita in view of Black disclose the method and the transponder-reader transaction system of claims 1 and 35, Kita discloses wherein said facial scan sensor (176) is configured to log at least one of a detected facial scan sample, processed facial scan sample and stored facial scan sample (column 5 lines 55 to column 6 line 43; column 9 line 66 to column 10 line 13).

Referring to Claim 5, Kita in view of Black disclose the transponder-reader transaction system of claim 1, Kita discloses further including a database (154) (i.e. organic authentication registration data) configured to store at least one data packet (i.e. authentication data), wherein said data packet (i.e. authentication data) includes at least one of proffered and registered facial scan samples, proffered and registered user information, terrorist information, and criminal information (column 10 line 62 to column 11 line 14; column 12 line 6 to 67; see Figures 10-15).

Referring to Claim 6, Kita in view of Black disclose the transponder-reader transaction system of claim 5, Kita discloses wherein said database (154) (i.e. organic authentication registration data) is contained in at least one of the transponder (151), transponder reader, sensor, remote server, merchant server and transponder-reader system (column 10 line 62 to column 11 line 14; column 12 line 6 to 67; see Figures 10-15).

Referring to Claim 7, Kita in view of Black disclose the transponder-reader transaction system of claim 6, Kita discloses wherein said remote database (154) (i.e. organic authentication registration data) is configured to be operated by an authorized sample receiver (356) (i.e. a radio

transmission/reception) (column 10 line 62 to column 11 line 14; column 16 lines 42 to column 17 line 39; see Figures 10-15 and 20).

Referring to Claims 8 and 37, Kita in view of Black disclose the method and the transponder-reader transaction system of claims 1and 35, Black discloses wherein said facial scan sensor device (2) (i.e. biometric sensor) is configured with at least one of an optical scanner and video camera (column 4 line 31 to 43; column 7 lines 42 to 67; see Figures 1-3 and 16-17).

Referring to claims 10, 32, and 42, Kita in view of Black disclose the method for of claims 1, 22, and 35, Black discloses wherein said step of proffering a facial scan to a facial scan sensor communicating with said system further comprises using said facial scan sensor to detect at least one of pupil dilation, pressure (i.e. force sensors), motion, and body heat (column 4 lines 31 to 43; see Figures 16).

Referring to Claims 11, 43 and 45, Kita in view of Black disclose the transponder-reader transaction system of claims 6 and 35, Kita discloses further including a device (152) (i.e. a control circuit) configured to compare a proffered facial scan sample (i.e. organic data input) with a stored facial scan sample (178) (i.e. registered biometric data) (column 12 lines 6 to 67; see Figure 15).

Referring to Claims 12 and 47, Kita in view of Black disclose the transponder-reader transaction system of claims 11 and 35, Kita discloses wherein said device (152) (i.e. a control

circuit) configured to compare a facial scan sample (i.e. authentication data) is at least one of a third-party security vendor device and protocol/sequence controller (column 12 lines 6 to 67; see Figure 15).

Referring to Claim 13, Kita in view of Black disclose the transponder-reader transaction system of claim 11, Kita discloses wherein a stored facial scan sample comprises a registered facial scan sample (column 12 lines 6 to 67; see Figure 15).

Referring to Claim 14, Kita in view of Black disclose the transponder-reader transaction system of claim 13, Kita discloses wherein said registered facial scan sample (178) (i.e. registered biometric data) is associated with at least one of: personal information, credit card information, debit card information, savings account information, and loyalty point information (column 19 line 47 to 67; see Figure 25).

Referring to Claim 15, Kita in view of Black disclose the transponder-reader transaction system of claim 14, Kita discloses wherein different registered facial scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, and loyalty point information (column 19 line 47 to 67; see Figure 25).

Referring to Claim 16, Kita in view of Black disclose the transponder-reader transaction system of claim 14, Kita discloses wherein a facial scan sample (i.e. authentication data) is

primarily associated with at least one of first user information (i.e. first authentication registration input) wherein said first information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, and wherein a facial scan sample is secondarily associated with at least one of second user information (i.e. first authentication registration input), wherein said second information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, where second user information is different than first user information (column 9 line 49 to column 10 line 13; column 19 line 48 to 67; see Figures 9 and 25).

Referring to Claim 17, Kita in view of Black disclose the transponder-reader transaction system of claim 14, Kita discloses wherein said transponder-reader transaction system is configured to begin mutual authentication upon verification of said proffered facial scan sample (column 16 lines 47 to column 17 line 25; see Figure 25).

Referring to Claim 18, Kita in view of Black disclose the transponder-reader transaction system of claim 14, Kita discloses wherein said transponder is configured to deactivate (i.e. end the process of verification) upon rejection (i.e. not coincident) of said proffered facial scan sample (column 7 line 53 to column 8 line 23; see Figures 6-8.

Referring to Claim 19, Kita in view of Black disclose the transponder-reader transaction system of claim 14, Kita discloses wherein said sensor is configured to provide a notification upon detection of a sample (column 5 line 40 to column 6 line 23; see Figure 5).

Referring to Claim 20, Kita in view of Black disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction (column 19 line 48 to 67; see Figure 25).

Referring to Claim 21, Kita in view of Black disclose the transponder-reader transaction system of claim 1, Kita discloses wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure (column 19 line 48 to 67; see Figure 25).

Referring to claim 23, Kita in view of Black disclose the method for of claim 22, Kita discloses further comprising registering at least one facial scan sample (i.e. authentication data) with an authorized sample receiver (8) (column 9 line 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 24, Kita in view of Black disclose the method for of claim 22, Kita discloses wherein said step of registering further includes at least one of: contacting said authorized sample receiver (32) (i.e. a wireless transmission reception section), proffering a facial scan to said authorized sample receiver (32), processing said facial scan to obtain a facial scan sample (i.e. authentication data), associating said facial scan sample (i.e. authentication data) with user information, verifying said facial scan sample (i.e. authentication data), and storing said facial scan sample upon verification (column 9 lines 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 25, Kita in view of Black disclose the method for of claim 22, Black discloses wherein said step of proffering includes proffering a facial scan to at least one of an optical scanner and video camera (column 4 lines 31 to 43; column 21 line 64 to column 22 line 12).

Referring to claims 26 and 38, Kita in view of Black disclose the method for of claims 22 and 35, Kita discloses wherein said step of proffering further includes proffering a biometric (i.e. fingerprint) to a biometric sensor (8) communicating with said system to initiate at least one of: storing, comparing, and verifying said biometric sample (i.e. authentication data) (column 9 lines 66 to column 10 line 59; column 11 line 15 to 61; see Figures 10-11).

Referring to claim 27, Kita in view of Black disclose the method for of claim 22, Kita discloses wherein said step of proffering a facial scan to a facial scan sensor (8) communicating with said system to initiate verification further includes processing database information (i.e. authorized data in an organic authentication registration data), wherein said database information (registration data) is contained in at least one of a transponder (151) (i.e. a equipment) (column 10 line 63 to column 11 line 61; see Figures 10-11).

Referring to claim 28, Kita in view of Black disclose the method for of claim 22, Kita discloses wherein said step of proffering a facial scan to a facial scan sensor (8) communicating with said system to initiate verification further includes comparing a proffered biometric sample (i.e. authentication data) with a stored biometric sample (i.e. organic authentication registration data registered in the organic authentication registration data unit 154) (column 11 line 42 to 61; see Figures 10-11).

Referring to claim 29, Kita in view of Black disclose the method for of claim 28, Kita discloses wherein said step of comparing includes comparing a proffered biometric sample (i.e. authentication data) to a stored biometric sample (i.e. registration data) by using at least one of a third-party security vendor device (37) (i.e. service business) and protocol/sequence controller ((152) (i.e. a control circuit) (column 5 line 40 to column 7 line 52; column 10 line 62 to column 11 line 67; see Figure 1-7 and 10-11).

Referring to claim 32, Kita in view of Black disclose the method for of claim 22, Black discloses wherein said step of proffering a facial scan to a facial scan sensor communicating with said system further comprises using said facial scan sensor to detect at least one of pupil dilation, pressure (i.e. force sensors), motion, and body heat (column 4 lines 31 to 43; see Figures 16).

Referring to claims 33 and 41, Kita in view of Black disclose the method for of claim 22 and 35, Kita discloses wherein said step of proffering a biometric to a biometric sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered biometric sample (i.e. authentication data) (column 9 line 66 to column 10 line 36).

Referring to claim 34, Kita in view of Black disclose the method for of claim 22, Kita discloses wherein said step of proffering a biometric to a biometric sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure (i.e. second authentication input section) (column 10 line 50 to 60; column 11 line 42 to column 12 line 4; see Figures 9-11).

Referring to claim 46, Kita in view of Black disclose the method for of claim 35, Kita discloses wherein said step of verifying includes verifying a proffered biometric sample using information contained on at least one of a local database (i.e. an organic authentication registration data at the equipment 154) (column 11 line 42 to 61; see Figure 10).

Claims 9, 30-31 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kita (US# 6,703,918) in view of Black (US# 6,307,956) as applied to Claims 1, 28 and 43, and in further view of Prokoski (US# 6,496,594).

Referring to claims 9, 30-31 and 44, Kita in view of Black disclose the method for of claims 1, 28 and 43, however, Kita in view of Black did not explicitly disclose wherein said facial scan sensor device is configured to detect and verify facial scan characteristics including at least one of nodal points, the distance between the eyes, the width of the nose, the jaw line, and the depth of the eye sockets.

In the same field of endeavor of comparing images of the face, Prokoski teaches that facial scan sensor device is configured to detect and verify facial scan characteristics including at least one of nodal points, the distance between the eyes, the width of the nose, the jaw line, and the depth of the eye sockets (column 12 line 28s to 64; see Figures 1 to 10) in order to obtain the verification of the same person.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize the need for detecting and comparing nodal points includes the distance between the eyes of Prokoski in the biometric comparison of Kita because comparing nodal points would improve the reliable and accurate verification of the same person that has been shown to be desirable in the portable authentication device of Kita in view of Black.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kinsella (US# 6,914,517) disclose a fingerprint sensor with feature authentication.

Hamid et al. (US# 6,877,097) disclose a security access method and apparatus.

Glass et al. (US# 6,332,193) disclose a method and apparatus for security transmitting and authenticating biometric data over a network.

Black (US# 6,307,956) discloses a writing implement for identity verification system.

Pare, Jr. et al. (US# 6,154,879) disclose a tokenless biometric ATM access system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 571-272-3061. The examiner can normally be reached on Mon-Fri, 8:30AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 571-272-3068. The fax phone numbers for the organization where this application or proceeding is assigned are 571-273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nam Nguyen
November 27, 2005

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600